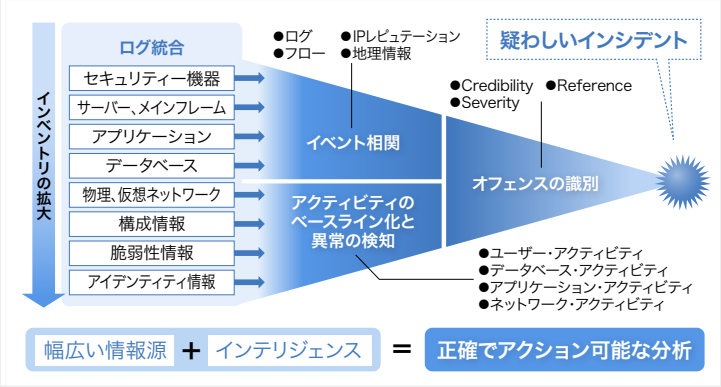
お客様事例

クラウド上のSIEM（Security Information and Event Management）を活用し、研究活動に制約を生じさせないセキュリティー・コントロールの効率化を実現

世界の多くの国や地域から集まった学生と教職員が研究活動に取り組んでいる沖縄科学技術大学院大学（以下、OIST）は、多様な文化的背景を持つ学生と教職員に対して厳しい制約を課すのではなく、ストレスを感じさせない快適かつ柔軟なシステム環境を提供することを目指し、早くからSIEMを活用してきました。しかし、オンプレミスで稼働する既存のSIEM製品は、日々の運用に多大な手間がかかるという課題を抱えていました。そこで新たに導入したのが、クラウド・サービスとして利用できるIBM QRadar on Cloudです。多種多様なイベント・ログの統合監視とリアルタイムでの相関分析によるセキュリティーの一次対応を、最小限の負荷で支えています。

［導入製品・サービス］ ● IBM QRadar on Cloud ● IBM QRadar Advisor with Watson



課題

- 多彩な研究活動を支えるため、厳しい制約を課すのではなく最低限かつ効果的なセキュリティー・コントロールによって安全性を担保
- オンプレミスで稼働する既存のSIEMでは、OSのアップデート、ストレージ管理、パフォーマンス管理など運用面での大きな負担が発生

ソリューション

- クラウド・サービスとして利用し、広範なシステムや機器から発生するイベント・ログを、できる限りカスタマイズすることなく取り込むことができるSIEM

効果

- セキュリティーの一次対応をIBM QRadar on Cloudに任せ、セキュリティー責任者はその先のより深い脅威の分析や、ユーザーとのコミュニケーションに専念
- SIEMを稼動させるために必要なサーバーなどのハードウェア導入、およびそれらの運用管理のために費やしていたワークロードやコストを削減

[お客様の課題]

最低限かつ効果的なセキュリティー・コントロールで多彩な研究活動の安全性を担保

OISTには現在、世界の多くの国と地域から集まった152人の学生および約870名の教職員が在籍しており、英語を公用語として、最先端のITと機器を利用した高度な研究活動が行われています。

そうしたOISTでの多彩な研究活動を支援する上で最も重要なことは、システムを使用するユーザーにストレスを感じさせない、快適かつ柔軟なシステム環境を提供することです。

OISTの最高情報セキュリティ責任者を務める永瀬 啓太氏は、「多様な文化のバックグラウンドを持ち、多岐にわたる研究テーマに取り組む学生や教員に対して厳しい制約を課すのではなく、最低限かつ効果的なセキュリティー・コントロールによって安全性を担保しなければなりません。また、ITリテラシーのレベルの異なる職員に対して情報セキュリティーの脅威を効率的に伝えるために、できる限りわかりやすくリスクを可視化するとともに、具体例を提示するなどコミュニケーションを工夫しています」と話します。

そうした中で、サイバー攻撃に関するイベント・ログを網羅的に収集・分析し、さまざまな脅威をリアルタイムに検知して速やかに対応するというセキュリティー対策の基本方針を講じ、早くからSIEMを活用してきました。

しかし、これまで利用してきたSIEM製品はオンプレミスで稼働するタイプのもので、管理サーバーのOSアップデートやストレージ管理、パフォーマンス管理など、運用面での大きな負担が生じていました。「学内でセキュリティー対策の専任者は実質的に私1人しかおらず、日々のSIEMの運用業務に多くの時間を割かれ、本来の脅威に対する監視や分析が手薄になってしまうことを懸念していました」と永瀬氏は話します。

> セキュリティーの一次対応はIBM QRadar on Cloudに任せるという前提で、私はその先のより深い脅威の分析や、ユーザーとのコミュニケーションに専念できるようになりました。

沖縄科学技術大学院大学
最高情報セキュリティ責任者
永瀬 啓太氏

[ソリューション]

多様なシステムのイベント・ログをカスタマイズすることなく取り込める

このような課題を解決するため、OISTが求めたのがクラウドをベースとしたSIEMのソリューションです。そうした中で目に留まったのがIBM QRadar on Cloudで、2017年12月よりPoC（概念実証）を開始し、2018年1月に導入を正式決定しました。

「クラウドに対応したいくつかのSIEM製品を調査しましたが、外部の脅威情報をリアルタイムで取り込めること、本学で利用している多様なシステムのイベント・ログをできる限りカスタマイズすることなく取り込めること、アラートやレポートのテンプレートが豊富に用意されていること、システムのキャパシティーを必要に応じて容易に増減できることなど、IBM QRadar on Cloudの総合力が選定の決め手となりました」と永瀬氏は話します。

そして現在、IBM QRadar on CloudにはファイアウォールやIDSをはじめとするネットワーク機器のイベント・ログ、学内のいたるところで分散稼動する数百台におよぶWindowsサーバーやLinuxサーバーのイベント・ログ、Office 365のアクセス・ログ、さらに別途導入したアンチウイルスや脆弱性スキャナーによる解析結果などがすべて取り込まれており、統合監視とリアルタイム分析を行っています。

「このように私たちが監視対象とするログは多岐にわたりますが、IBM QRadar on Cloudが標準で備えている基本ルールをほぼそのまま適用することができ、約1カ月という短期間で既存のSIEMからの移行作業を完了し、本番運用を始めることができました。若干の

誤検知はあるもののほとんど問題にならないレベルで、早急に対応しなければならない脅威を高精度に洗い出してくれています」と永瀬氏は話します。

加えてOISTが高く評価しているのが、IBM QRadar on Cloudのプラグ・イン・アプリケーションとして提供されているIBM QRadar User Behavior Analytics（以下、UBA）機能です。これはMicrosoft Active Directoryと連携してユーザーの通常時と異なる行動を監視するもので、通常ありえない時間帯にアクセスしていたり、過去になかったサーバーへのアクセスがあったり、ログイン認証を数回にわたり失敗しているなど、ユーザーの不審な振る舞いや通常から逸脱した動作を検出してアラートを発します。

「従来のSIEMでもユーザーのログイン/ログオフやアクセス・ログを記録していましたが、通常よりもログイン回数が〇〇%以上上限したといった単純なしきい値でしか異常を判断することができず、脅威の分析や内部不正に対する効果的な対策には至っていませんでした。UBA機能を活用することで、ユーザーの変則的な行動を自動的に検知することが可能となりました」と永瀬氏は話します。

【効果/将来の展望】

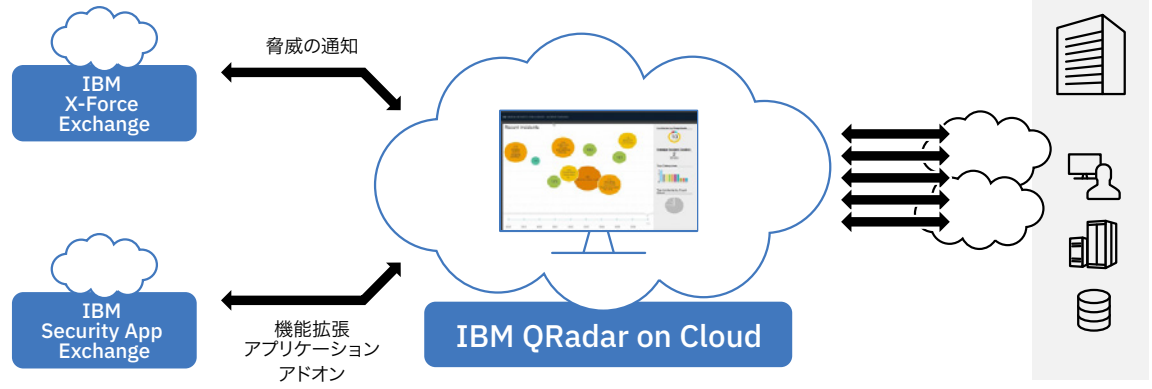
レピュテーションIPの背後にひそむ脅威の根本原因をWatsonテクノロジーで分析

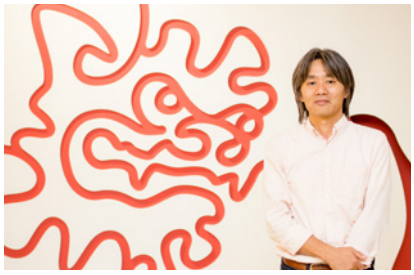
IBM QRadar on Cloudを導入することで、即座に実感したのがセキュリティー運用に関する作業負荷軽減の効果です。

「オンプレミスで運用していた従来のSIEMで手を煩わされていた、OSのメンテンスやシステムの稼働監視などは不要となりました。IBM QRadar on Cloudから毎日届けられるレポートを確認し、リアルタイムのアラートに対応するだけで済むため、ほとんど手間はかかりません。セキュリティーの一次対応はIBM QRadar on Cloudに任せるという前提で、私はその先のより深い脅威の分析や、ユーザーとのコミュニケーションに専念できるようになりました」と永瀬氏は話します。

また、クラウド・サービスとして利用できるIBM QRadar on Cloudでは、従来のオンプレミスのSIEMで不可欠だったサーバーやストレージなど、SIEM を稼動させるためのシステムの導入および維持管理に費やしていたコストも削減されています。

IBM QRadar on Cloud 活用イメージ





これらのメリットを高く評価しつつ、OISTはIBM QRadar on Cloudの活用範囲をさらに拡大しています。その1つがIBM QRadar Advisor with Watsonとの連携です。

従来のSIEMでもレピュテーションIPやセキュリティー・ベンダーから配信される脅威情報を定時的にダウンロードしてシステムに取り込み、検知したセキュリティー・イベントと照らし合わせて分析することで、サイバー攻撃のリスクをある程度判定することは可能でした。

しかし、この手法はアンチウイルス・ソフトウェアの定義ファイルに相当する仕組みに基づいて既知の脅威を検知しているにすぎず、昨今の多様化・巧妙化するサイバー攻撃のパターンを考慮すると、次々に出現する未知の脅威への対策は後手に回ってしまうことが懸念されました。また、提供される分析結果も、既知の脅威情報にマッチしたかどうかがアラートやレポートとして表示されるのみでした。

「IBM QRadar Advisor with Watsonを利用したところ、外部のリアルタイムの脅威情報を用いて検知したセキュリティー・イベントを分析することが可能となりました。レピュテーションIPの背後にどんな脅威がひそんでいるのか、その根本原因とともに、なぜそれを脅威と判定したのかという根拠を示すことも可能で、発生したインシデントに対する初動時間を大幅に短縮することができました」と永瀬氏は話します。

さらに今後に向けてOISTでは、現在は別ソリューションとして運用している脆弱性スキャナーの実装、ネットフローの分析、インシデントを管理するチケット・システムとの連携、IDカードによる入退室管理をはじめとする物理セキュリティー・システムからのログの取り込みなどを検討。IBM QRadar on Cloudをプラットフォームとしたセキュリティー対策の拡張と高度化を推進しています。

OIST 沖縄科学技術大学院大学

沖縄科学技術大学院大学

〒904-0495 沖縄県国頭郡恩納村字谷茶1919-1
https://www.oist.jp/ja

沖縄の自立的発展と世界の科学技術向上に寄与することを目的に、2011年11月1日に設立された政府からの財政支援も受ける5年一貫制の博士課程を置く大学院大学。現在、39の国と地域から152人の学生が在籍するとともに、世界の50を超える国と地域から集まった教職員約870名が日々教育研究活動に従事。公用語は英語で、学生たちは最先端の研究機器を利用しながら高度な研究活動を行っています。

〒103-8510 東京都中央区日本橋箱崎町19-21